

APPENDIX

Customer Premise Equipment (CPE) Settings for Direct Connection Scenario

End-Point Settings.

1. H.323 endpoints are configured with IP address of Video Switch as call mediation system (i.e.) H.323 gatekeeper or (Session Initiation Protocol) SIP proxy. Endpoints use these IP address for registration (using e.g. H.323 RAS signaling) and call initiation (using e.g. H.323 ARQ signaling).
2. Users optionally authenticate themselves with H.323 gatekeeper/SIP proxy.

Enterprise Edge Router Settings

1. Enterprise edge router supporting the dedicated connection is configured to allow traffic that has the endpoint and video switch IP addresses as the source/destination IP addresses to pass.

Customer Premise Equipment (CPE) Settings for DSL connection Scenario

End-Point Settings.

1. H.323 endpoints are configured with IP address of Video Switch as call mediation system (i.e.) H.323 gatekeeper or (Session Initiation Protocol) SIP proxy. Endpoints use these IP address for registration (using e.g. H.323 RAS signaling) and call initiation (using e.g. H.323 ARQ signaling).
2. Users optionally authenticate themselves with H.323 gatekeeper/SIP proxy.

Enterprise DSL Integrated Access Device (IAD) Settings

1. Creation of separate ATM Permanent Virtual Circuit (PVC) or Frame Relay (FR) Data Link Communication Identifier (DLCI) circuit for video traffic destined to the Video Switch.
2. (Optionally) prioritizing processing and delivery of video PVC/DLCI traffic.

Customer Premise Equipment (CPE) Settings for Firewall Traversal Scenario

End-Point Settings.

1. H.323 endpoints are configured with IP address of Enterprise Video Gateway as call mediation system (i.e.) H.323 gatekeeper or (Session Initiation Protocol) SIP proxy and H.323/SIP application gateway firewall. Endpoints use these IP address for registration (using e.g. H.323 RAS signaling), call initiation (using e.g. H.323 ARQ signaling), and forwarding audio/video (using e.g. RTP/RTCP protocols) data.
- 2.
3. Users optionally authenticate themselves with H.323 gatekeeper/SIP proxy.

Enterprise Video Gateway Settings

1. Setting a globally routable (i.e. not a private unregistered) IP address for the Enterprise Video Gateway at install time.
2. Setting up of secure (i.e. authenticated and optionally encrypted) IPSEC-based communication channel between Enterprise Video Gateway and Video Switch.
3. Turning on of H.323/SIP "Pseudo" call mediation and firewall modules. The function of these "pseudo" modules is to appear as H.323/SIP call mediation and firewall systems to end-points. It

replaces its IP address with the IP address(es) of the H.323/SIP call mediation and firewall modules on the Video Switch for traffic received from endpoints, encapsulates such traffic in IPSEC traffic, and forwards it to the Video Switch.

Enterprise Edge Router Settings

1. Enterprise firewall is configured to allow traffic across IPsec port from/to Enterprise Video Gateway and Video Switch(es).
2. Enterprise edge router is optionally configured to prioritize delivery of video traffic by adding Diff-Serv labels to video traffic destined for Video Switches.

Video Switch Settings

Per-Enterprise Subscriber Settings

Tunneling Services

1. *Creation of IPSEC tunnels between Video Switch and Enterprise Video Gateways located in each subscriber network (optional).* This requires setting up of IPSEC authentication and encryption parameters on Video Switch. The tunneling service unencapsulates traffic from Enterprise Video Gateways. It also maintains a dynamic mapping of IP address of each Enterprise Video Gateway and port numbers so that the Enterprise Video Gateway can correctly route call setup and video traffic back through to the appropriate Enterprise Video Gateway.

Routing Services

1. *Creation of a virtual router within Video Switch for each subscriber (required).* A subscriber may have multiple virtual routers within a switch (e.g. for different physical locations supported by the same switch). The definition of a virtual router is based on the Enterprise Video Gateway IP address information (in case of video traffic traversing firewalls), enterprise edge router or DSL IAD IP address information, the Video Switch physical network interface that is used (in case of a dedicated connection) or the POP edge/aggregation router (in case of a video traffic traversing firewalls) for traffic from/to subscriber enterprise. Virtual routers are at the heart of the services segmentation and layering architecture of the video services switch.
2. *Configuring of routing services for each enterprise subscriber (required).* This involves support of BGP and OSPF routing on a per-virtual router basis (i.e. separate routing tables are maintained for each subscriber to segment its traffic).

Addressing Services

3. *Configuring of H.323 gatekeeper and/or SIP proxy services for each subscriber served by Video Switch(required).* For H.323 gatekeeper services, this includes the following steps: Starting gatekeeper services, configuring each subscriber as a H.323 “zone” in the gatekeeper, enabling gatekeeper discovery/registration of endpoints, configuring H.323 security, configuring inter-gatekeeper communication, creation of call records/logs for billing and administrative purposes. Etc.

Security Services

4. *Configuring of H.323/SIP firewall services (optional).* Configuring of H.323/SIP application proxy firewall services by each enterprise subscriber. The H.323/SIP parses the control flows to dynamically open/close ports for control traffic. It forwards this information to the network data plane hardware. The configuring step includes addition of firewall address information into the gatekeeper database for that zone, setting of ports or channels that are statically open (by default the firewall is an opaque system) and security logging.
5. *Configuring of H.323/SIP NAT Services (optional).* First, it parses the packet header and payload of Q.931/H.245 control (i.e. call setup) streams and substitutes non-routable endpoint source IP addresses and port numbers with its own globally unique H.323 proxy IP address and port numbers and vice versa (storing the IP address/port number mapping information as it does so). Second, it substitutes the IP addresses in the header of the RTP data streams substituting non routable source IP addresses with its own H.323 proxy IP address and vice versa.

6. *Configuring of Encryption Services (optional)*. Configuring of use of encryption by enterprise subscriber and destination IP address (enterprise want to have encrypted communication with only some of their partners etc).
7. *Configuring of MPLS/BGP VPN Services (optional)*. The benefit of the Video Switch supporting MPLS VPNs services is that it enables video-specific VPNs across ATM, IP and L2-type backbone networks. Second, membership of MPLS VPNs can be dynamically updated enabling simplified creation of extranet and intranet VPNs. This requires configuring of each subscriber virtual router with MPLS VPN capability including creation of VPN route/forwarding tables, configuring BGP Routing Sessions, Configuring virtual router to Provider Edge Routing Sessions, Configuring RIP/BGP/Static virtual router to Customer Edge Routing Sessions (MPLS VPN RFC Reference).

QoS Services

8. *Configuring of Bandwidth Management Services (optional)*. This enables setting of maximum video bandwidth allowed into or from an enterprise subscriber by time of day.
9. *Creation of MPLS Traffic Engineering Paths*. The benefit of Video Switch supporting MPLS TE is that it enabled creation of premium-priced guaranteed bandwidth paths for video flows across an SP MPLS backbone. This requires configuring of MPLS tunnels, enabling of express forwarding and enabling IS-IS routing (MPLS TE RFC reference).
10. *Configuring of Diff-Serv QoS Services (optional)*. Configuring of TOS/IP Precedence field for video traffic (i.e. RTP streams) to/from each enterprise. This enabled core devices in an SP network to give prioritized treatment to video traffic.
11. *Configuring of IP over ATM QoS Services (optional)*. IP over ATM services (RFC 2684) are configured on a per-virtual router and per-physical interface basis.

12. *Video Jitter Buffer Configuration*. Configuration of size of jitter buffer within Video Switch on a per-enterprise subscriber basis.

Per-Enterprise Users Settings

User-level Policy Services

These services include: incoming or outbound calling, allowable max. video codec (quality) level, Audio or audio/video, time of day, calling priority among users in a subscriber corporation, and Time of day restrictions.

Switch Management Capabilities.